DETAILED ACTION

The instant application having Application No. 10/534,541 is presented for examination by the examiner. Claims 1, 3-10, 12, 14, 15, and 17-25 are pending.

Response to Amendment

Claim Objections

The current amendments overcome the previous claim objections.

Response to Arguments

Applicant's arguments filed 12/19/09 with respect to claims 12 and 14 have been fully considered but they are not persuasive. The following interpretation of the prior art is solely based on the current set of claims and arguments submitted by the Applicant. It is not the only possible interpretation of the prior art and may be altered when/if the claims and/or arguments change.

Applicant alleges that claims 12 and 14 are not obvious in view of Newcombe and Arnold because they fail to teach the key information generating means and the user authentication information transmitting means which transmits user authentication information along with the key information to the authentication server. The argument is moot because the specific feature of transmitting a public key of the user along with the authentication information to the authentication server is relied upon from the teaching of Medvinsky as explained below.

Applicant's arguments with respect to claims 7, 21, and 22 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments with respect to claims 1, 15, and 23 have been considered but are moot because those rejections have been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7-10, 12, 14, 21, 22, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Newcombe** (US 2003/0172269 A1) in view of Arnold et al. (WO 03/055170 A1), hereinafter **Arnold** and in view of Application Publication 2003/0163693 to **Medvinsky**.

As per claim 7, Newcombe teaches the limitation of an "authentication server in an authentication system in which an authentication of a user utilizing a user terminal is performed through the user terminal by an authentication server and a request is made to an application server to provide a service on the basis of the authentication" (Fig. 1; page 2, paragraph 0025) as the system includes a client that desires access to a

content server, application server, or the like. The authentication manager includes an application authentication server and ticket granting server.

Further, Newcombe teaches the limitation of "a reception means for receiving an authentication request inclusive of a user authentication information transmitted from the user terminal" (page 3, paragraph 0044) as Application Authentication Server (AAS) is configured to authenticate a user. Where, (page 4, paragraph 0052) clients are enabled to request access to servers, such as content servers by requesting content tickets from AAS. Clients are enabled to provide information associated with local and remote IP addresses to AAS as part of the request for content tickets.

Furthermore, Newcombe teaches the limitation of "an authentication means to which the user authentication information of the received authentication request is input and which authenticates the user on the basis of the user authentication information and providing a signal indicating a successful authentication upon a successful authentication" (page 5, paragraph 0064) as Authentication Server (AS) determines the user is a valid user and provides client with a Ticket Granting Ticket. Where AS is a part of AAS (page 4, paragraph 0054) and (page 10, paragraph 0115) a signal is provided that indicates whether the client is authentic or not.

Additionally, Newcombe teaches authentication information generating means for generating information-for-authentication using at least the allocated address and the key information (0025 and 0029).

In addition, Newcombe teaches the limitations of "a ticket issuing means for issuing a ticket containing the allocated address, the key information, and the

information-for-authentication" (0025) and "and a ticket transmitting means to which the ticket is input and which transmits the ticket to the user terminal" (page 4, paragraph 0044) as Application Authentication Server (AAS) is configured to provide the authenticated user one or more content tickets that enables authenticated user to access one or more content servers. The content ticket includes (page 4, paragraph 0048) the client's local and remote IP addresses.

It is noted, however, that Newcombe does not teach the limitation of "an address allocating means for allocating an address to the user terminal in response to an input of the signal indicating a successful authentication of the user."

On the other hand, Arnold teaches the abovementioned limitation (page 5, lines 25-29) as an IP address is assigned to the user/subscriber during the single sign-on authentication procedure performed in the network of the respectively underlying network service provider of the user or the like.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Arnold into the system of Newcombe to allow the AAS to keep full control of the IP address assignment process in view of the limited pool of available IP addresses.

Newcombe is silent in explicitly disclosing that the public key of a user is sent to the server in the request. Medvinsky teaches a ticket granting protocol in which the client and server perform a Diffie-Hellman exchange that includes each side sending their respective public key to the other side (0030-31). Thus the client sends its public key to the server. This is down so they two sides may establish a secret key without

having to secretly exchange a shared key. Newcombe teaches using asymmetrical keys under RSA to secure the transmissions. Substituting a Diffie-Hellman key exchange for an RSA exchange in within the ordinary capabilities of one skilled in the art. The claim is obvious because one of ordinary skill in the art can substitute known elements which produce predictable results.

With respect to claim 8, Newcombe teaches the limitation of "an authentication information generating means for generating an authentication information for information which includes at least the allocated address using a shared secret key which is beforehand shared between the authentication server and the application server" (page 4, paragraph 0044) as Application Authentication Server (AAS) is configured to provide the authenticated user one or more content tickets that enables authenticated user to access one or more content servers. The content ticket includes (page 4, paragraph 0048) the client's local and remote IP addresses. Furthermore, (page 5, paragraph 0065) the client readable portion [of the ticket] is signed with the private key of the authentication server.

With respect to claim 9, Newcombe teaches the limitation of "the authentication server comprises a user identifier allocating means for allocating a user identifier which corresponds to the authenticated user in response to the authentication request for a

successful authentication of the user" (page 4, paragraph 0057) as Authentication Server (AS) is enabled to authenticate a user.

In addition, Newcombe teaches the limitations of "authentication information generating means is configured to process the information including the allocated address, the key information, and the user identifier to produce information for authentication and the ticket issuing means is configured to combine at least the information for authentication, the allocated address, the key information and the user identifier to form the ticket" (0025) and "and a ticket transmitting means to which the ticket is input and which transmits the ticket to the user terminal" (page 4, paragraph 0044) as Application Authentication Server (AAS) is configured to provide the authenticated user one or more content tickets that enables authenticated user to access one or more content servers. The content ticket includes (page 4, paragraph 0048) the client's local and remote IP addresses.

As per claim 10, Newcombe teaches the user identifier allocating means is configured to encrypt information which directly identifies the user by using an identifier generating secret key of the authentication server to produce the user identifier (0065).

As per claim 12, Newcombe teaches a user terminal in an authentication system in which an authentication of a user utilizing a user terminal is performed by an

authentication server and a request to provide a service is made to an application server on the basis of the authentication (0052), comprising:

a ticket reception means for receiving a ticket transmitted from the authentication server (0064), key information (0029) and information-for-authentication produced by using at least the allocated address and the key information (0065);

a session establishing means to which the ticket is input and which transmits a first packet including the ticket to the application server for establishing a session with the application server (0047);

a service request means for transmitting a second packet representing a service request to the application server through the established session (0046);

a key information generating means to which a public key of the user terminal is input (0025 and 0029);

and a packet cryptographic processing means to which a packet to be transmitted from the user terminal and the session secret key are input and which applies a processing to the transmitted packet which guarantees that there is no forgery in the packet by the session secret key (0065);

a user authentication information transmitting means configured to transmit the user authentication information to the authentication server (0052 and 0072).

It is noted, however, that Newcombe does not teach the limitations of "an address allocating means for allocating an address to the user terminal for a successful authentication of the user", "means for setting up an address contained in the ticket as a source address for a packet which is to be transmitted from the user terminal."

On the other hand, Arnold teaches the abovementioned limitation (page 5, lines 25-29) as an IP address is assigned to the user/subscriber during the single sign-on authentication procedure performed in the network of the respectively underlying network service provider of the user or the like.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Arnold into the system of Newcombe to allow the AAS to keep full control of the IP address assignment process in view of the limited pool of available IP addresses.

Newcombe is silent in explicitly teaching the key information represents the public key of the client and that is sent along with the user authentication information and the session keys are created using the private and public keys of the user terminal and the application server. Newcombe does teach using a session key between the client and server and that any algorithm could be used. The algorithm used in the claim is a well known Diffie-Hellman type (e.g. IKE, Oakley) key exchange. Medvinsky teaches this same type of key exchange with the use of tickets (0013). As taught by Medvinsky, it is necessary to send the public key of the client to the server in order to complete a Diffie-Hellman type key exchange (0030-31). It is obvious to one of ordinary skill to substitute known methods which produce predictable results. The combination of Medvinsky produces a well known and secure key exchange.

As per claim 14, Newcombe teaches a user terminal in an authentication system in which an authentication of a user utilizing a user terminal is performed by an

authentication server and a request to provide a service is made to an application server on the basis of the authentication (0052), comprising:

a ticket reception means for receiving a ticket transmitted from the authentication server (0064), key information (0029) and information-for-authentication produced by using at least the allocated address and the key information (0065);

a session establishing means to which the ticket is input and which transmits a first packet including the ticket to the application server for establishing a session with the application server (0047);

a service request means for transmitting a second packet representing a service request to the application server through the established session (0046);

a key information generating means to which an authentication purpose shared secret key (0029) which is shared with the application server and a random number (timestamp) which changes each time (0025) a session is established are input and which generates a key information by processing random number by the authentication purpose shared secret key (0031);

a key information generating means to which a public key of the user terminal is input and which generates a key information relating to the public key of the user terminal (0025 and 0029);

and a packet cryptographic processing means to which a packet to be transmitted from the user terminal and the session secret key are input and which applies a processing to the transmitted packet which guarantees that there is no forgery in the packet by the session secret key (0065);

a user authentication information transmitting means configured to transmit the key information together with the user authentication information to the authentication server (0052 and 0072);

the user authentication information transmitting means which is configured to transmit the user authentication information (0052 and 0072).

It is noted, however, that Newcombe does not teach the limitations of "an address allocating means for allocating an address to the user terminal for a successful authentication of the user", "means for setting up an address contained in the ticket as a source address for a packet which is to be transmitted from the user terminal."

On the other hand, Arnold teaches the abovementioned limitation (page 5, lines 25-29) as an IP address is assigned to the user/subscriber during the single sign-on authentication procedure performed in the network of the respectively underlying network service provider of the user or the like.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Arnold into the system of Newcombe to allow the AAS to keep full control of the IP address assignment process in view of the limited pool of available IP addresses.

Newcombe is silent in explicitly teaching the key information represents the public key of the client and that is sent along with the user authentication information and the session keys are created using the private and public keys of the user terminal and the application server. Newcombe does teach using a session key between the client and server and that any algorithm could be used. The algorithm used in the claim

is a well known Diffie-Hellman type (e.g. IKE, Oakley) key exchange. Medvinsky teaches this same type of key exchange with the use of tickets (0013). As taught by Medvinsky, it is necessary to send the public key of the client to the server in order to complete a Diffie-Hellman type key exchange (0030-31). It is obvious to one of ordinary skill to substitute known methods which produce predictable results. The combination of Medvinsky produces a well known and secure key exchange.

With respect to claim 21, it is rejected in view of the reasons stated in the rejection of independent claim 7.

With respect to claim 22, it is rejected in view of the same reasons as stated in the rejection of independent claim 12.

As per claim 25, Newcombe teaches the authentication server has a secret key and a public key for digital signature (0029), and said ticket issuing means comprises: an authentication information generating means for computing a digital signature on the information including at least the allocated address using the secret key to produce the information for authentication so that the application server can verify the presence or absence of any forgery in the information for authentication in the ticket using the public key of the authentication server (0030 and 0065-0066).

Allowable Subject Matter

Claims 1, 3-6, 15, 17-20, 23, and 24 are allowed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431